ABSTRACT

A method for issuing a certificate using biometric information in a public key infrastructure-based authentication system is provided. In the present invention, an authentication code used to protect a certificate issuance request message is assigned to a user by a certificate authority not at a registration step but at a certificate issuance request step where a user authentication is performed with user's biometric information. Therefore, there is no need for a user to remember and enter the complex authentication code to be issued the certificate, thereby simplifying certificate issuance procedures. Further, in the present invention, the authentication code is assigned to the user at the certificate issuance step only after a real-time authentication using the user's biometric information is performed. For this reason, even though a reference code of the user is revealed to a third party before the certificate issuance step, it can be prevented that the third party tries to be issued the certificate, thereby maintaining higher reliability when the certificate is issued.